Granskning av efterlevnaden av dataskyddsförordningen

Revisionsrapport

Alingsås kommuns revisorer

KPMG AB

Juni 2020

Antal sidor: 22

Innehållsförteckning

1 Sammanfattande bedömning och rekommendationer

Sammanfattningsvis kan konstateras att det finns utvecklingsområden och brister vad avser arbetet med och efterlevnaden av dataskyddsförordningen.

Revisionsrapporten är utifrån önskemål och behov även av vägledande karaktär, där nämnderna kan få ett stöd i det dagliga arbetet genom rapporten.

Sammantaget upplever vi intervjuade tjänstepersoner och politiker som engagerade och villiga att genomföra ett förbättrings- samt utvecklingsarbete vad gäller efterlevnaden av dataskyddsförordningen.

Mot bakgrund av vår granskning och iakttagelser bedömer vi att följande bör ses över:

Dagens upplägg med en kombinerad tjänst som digitaliseringsansvarig och dataskyddsombud inte är optimalt där tillägnad tid på ca 20 % inte är tillräcklig för uppdraget som dataskyddsombud för en kommun i Alingsås storlek. Vid tid för granskningen framkommer att det inte finns tid till att granska och kontrollera nämndernas och styrelsernas arbete, (vilket ska ske systematiskt), genomföra riktade utbildningsinsatser, kontinuerliga möten mellan dataskyddsombudet och förvaltningarna, kontinuerlig rådgivning mm.

- Vi bedömer att det finns ett behov av en kunskapsökning i förvaltningarna samt bland personal ute på fältet vad gäller **hantering, dokumentation** och **risk- och konsekvensbedömning** av personuppgiftsincidenter. Detta i syfta att bl.a. uppnå en enhetlig tolkning och förståelse i verksamheterna av dataskyddsförordningens krav och intentioner vad gäller personuppgiftsincidenter samt skapa förutsättningar för en korrekt hantering i den praktiska tillämpningen.

- Vi anser att det finns ett behov av ett omtag avseende dokumentation av personuppgiftsincidenter, där det finns ett behov av bl.a. en ökad central styrning vad gäller övergripande styrdokument följt av mallar/inrapporteringsblanketter. Vi bedömer att dokumentationen av förekommande incidenter inte är på en tillfredställande nivå, då dokumentationen är bristfällig.

  Dokumentation av personuppgiftsincidenter är obligatorisk, där den personuppgiftsansvarige ska dokumentera samtliga personuppgiftsincidenter inbegripet **omständigheterna kring incidenten**, **risker** och **effekter** samt de **korrigerande åtgärder** som har vidtagits. **Dokumentation ska ske oaktat** om nämnden bedömer att inrapportera personuppgiftsincidenten till Datainspektionen eller ej. Det bör framhållas att personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter samt förtroendeskador för kommunen.

  Det bör vidare noteras att anmälan till Datainspektionen är obligatorisk, såvida det inte är sannolikt att incidenten leder till en hög risk för fysiska personers rättigheter och friheter. Detsamma gäller information till de registrerade.

- En förklarande orsak avseende de nämnder som inte har angivit någon förekomst av personuppgiftsincidenter bedöms vara avsaknad av tillräckliga kunskap om vad en personuppgiftsincident är och vad som ska klassas som en incident.

  Vi anser att det finns ett behov av att förvaltningarna samt personal ute på fältet får en närmare information om klassning av personuppgiftsincidenter, där utveckling av begreppet följt av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

- I syfte att kunna genomföra en risk- och konsekvensbedömning följt av bedömning om lämpliga och korrekta åtgärder behöver nuvarande blankett kompletteras samt uppdateras, (se sid 14 för områden som bör tillföras).

- Rapporten för personuppgiftsincidenter bör kompletteras med ett förvaltningsbeslut om huruvida personuppgiftsincidenten ska inrapporteras till datainspektionen eller ej. rapport inklusive ett beslut bör diarieföras. Det bör betonas att samtliga incidenter som är kopplade till personuppgifter ska **dokumenteras, oaktat allvarlighetsgrad.**

- Vi bedömer att samtliga uppkomna personuppgiftsincidenter bör rapporteras till dataskyddsombudet. Dataskyddsombudets främsta uppdrag är att övervaka efterlevnaden av dataskyddsförordningen följt av rådgivning och stöd till personuppgiftsansvariga nämnder och bolagsstyrelser. Härigenom är det av vikt att information om eventuellt uppkomna personuppgiftsincidenter kommer till dataskyddsombudets kännedom.

- Vi rekommenderar att kommunstyrelsens ledamöter årligen får ta del av en statistik avseende inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt. I dagsläget når inte informationen till kommunstyrelsen i sin helhet.

- Vi bedömer att det krävs ett omtag vad avser arbetet med registerförteckningar, där det finns väsentliga brister. Det finns ett behov av översyn av strukturen i registerförteckningarna. Ett första steg bör därmed vara revidering av nuvarande mall för registerförteckningar vad gäller struktur och frågeställningar. Granskningen visar att utifrån befintliga brister i mallen har vissa nämnder skapat ”egna varianter”.

- Vi bedömer att det är av vikt att det finns uppdaterade kommunövergripande styrdokument följt av korrekta mallar och underlag avseende hantering av personuppgifter. Detta i syfte att uppnå en enhetlig nivå och hantering av behandling av personuppgifter inom verksamheterna.

- Vi bedömer vidare att det finns ett tydligt behov av utbildningsinsatser vad avser registerförteckningar som är grundstommen i hanteringen av personuppgifter.

- Respektive nämnd och styrelse är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Dock ska kommunstyrelsen inom ramen för sin uppsiktsplikt följa upp huruvida nämnder och

bolagsstyrelser hanterar det ålagda ansvaret följt av framtagande av centrala styrdokument som stödjer verksamheterna i dataskyddsarbetet.

- Registerförteckningarna ska uppdateras vid behov och hållas aktuella. Nämnderna har ett ansvar att tillse att samtliga personuppgiftsbehandlingar upptas i en registerförteckning. **Härigenom bör nämnderna sondera huruvida samtliga behandlingar finns registrerade.**

- Den gemensamma filytan bör ses över snarast, där hanteringen strider mot gällande lagstiftning.

- Det finns vidare lokala lagringsutrymmen, där anställda kan ha lagrat personuppgifter. Vi rekommenderar att samtliga anställda uppmanas att se över lokala lagringsutrymmen för att antingen flytta nödvändiga uppgifter för arbetet, till rätt plattform eller gallra. Det bör betonas att personuppgifter kan endast behandlas med stöd av rättsliga grunder, för specifika, konkreta och berättigande ändamål.

- Dataskyddsombudet bör genomföra dokumenterade granskningsinsatser för respektive nämnd och bolag. Resultatet följt av rekommendationer bör dokumenteras i en granskningsrapport för varje nämnd och styrelse.

- Kommunstyrelsen bör upprätta en dokumenterad rutinbeskrivning avseende rättelse och radering av personuppgifter. Av rutinen bör ansvarsfördelning samt praktiskt utförande vid en eventuell begäran om rättelse eller radering framgå.

*I samband med faktagranskningen har det framkommit att kommunstyrelsen kommer fr.o.m. september månad köpa en renodlad tjänst som dataskyddsombud från kommunalförbundet Göteborgsregionen. Detta bedöms som positivt.

2 Bakgrund

Vi har av Alingsås kommuns revisorer fått i uppdrag att granska kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen.

2.1 Syfte och revisionsfråga

Rapporten syftar till att granska kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen. Följande avser rapporten besvara:

1. Finns det ett centralt utsett dataskyddsombud?
2. Befinner sig dataskyddsombudet i en oberoendeposition?
3. Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
4. Har kommunstyrelsen säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskydds-förordningen?
5. Har kontroller av registerförteckningar genomförts för att säkerställa att förteckningarna är korrekt upprättade utifrån dataskyddsförordningens grundläggande principer? (Ändamålsbeskrivning, personuppgiftsansvarig, kategorier av personuppgifter, förekomst av känsliga personuppgifter, dokumentation om förekomst av överföring av personuppgifter sker till tredje land, mottagare internt och externt, tidsfrister för radering, rättslig grund för behandling, beskrivning av tekniska och organisatoriska säkerhetsåtgärder m.m.)
6. Finns rutiner för incidentrapporteringar?
7. Har rutinerna för incidentrapportering efterlevts av nämnder och styrelsen?
8. Hur många incidentrapporter har inkommit sedan lagens ikraftträdande?
9. Har riskbedömning genomförts av incidenterna och hur många har kategoriserats som allvarliga?
10. Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till Datainspektionen?
11. Finns dokumenterade rutiner för begäran om registerutdrag?
12. Finns dokumenterade rutiner för rättelse av uppgifter?

13. Finns dokumenterade rutiner för radering av uppgifter?

14. Har riktade utbildningar/information tillhandahållits till nämnderna utifrån verksamheternas särskilda behov vad gäller behandling av personuppgifter?

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
- Riktlinjer från European Data Protection Board, (Europeiska dataskyddsstyrelsen)
- Interna riktlinjer/policys

2.3 Metod

Studium och genomgång av relevanta styrdokument och beslutsunderlag samt övergripande granskning och analys av registerförteckningar avseende personuppgiftsbehandlingar.

Intervjuer och avstämningar har genomförts med digitaliseringsansvarig tillika dataskyddsombud, stabschef/administrativt chef, kommunjurist samt kommunstyrelsens ordförande.

Rapporten har faktagranskats av dataskyddsombudet samt stabschef/administrativ chef.

3. EU-rättslig lagstiftning

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för Dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av person-uppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgifts-ansvariga nämnder och styrelser.

Hantering av personuppgifter ska ske utifrån förordningens grundläggande principer enligt följande:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”**rättslig grund**”. Utan en rättslig grund är personuppgiftsbehandling ej laglig.

Vidare ska styrelsen och nämnderna utse ett dataskyddsombud, (DSO), som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen.

4. Dataskyddsombud

Dataskyddsförordningen, artikel 37.1, fastställer att ett dataskyddsombud, (DSO) ska utses i följande tre fall:

a) Behandlingen genomförs av en myndighet eller ett offentligt organ.

b) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning.

c) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter och personuppgifter som rör fällande domar i brottmål och överträdelser.

4.1 Dataskyddsombudets uppdrag

Enligt dataskyddsförordningen, artikel 39 ska dataskyddsombudet ha minst följande uppgifter:

- Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt dataskyddsförordningen.

- Att **övervaka och kontrollera** efterlevnaden av dataskyddsförordningen.

- Att övervaka och kontrollera efterlevnaden av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

- Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.

- Att samarbeta med tillsynsmyndigheten.

- Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, och vid behov samråda i alla andra frågor.

Europeiska dataskyddsstyrelsens riktlinjer fastställer att dataskyddsombudets främsta prioritering bör vara ett möjliggöra **efterlevnad** av dataskyddsförordningen.

Det är vidare av stor vikt att dataskyddsombudet befinner sig i en **oberoendeposition**, där vederbörande ska kunna arbeta självständigt och fullgöra sina uppgifter på ett oberoende sätt. Detta innebär att personuppgiftsansvariga eller personuppgiftsbiträden får exempelvis inte instruera dataskyddsombudet om vilka resultat som bör uppnås, hur ett klagomål ska hanteras eller att inta en viss ståndpunkt i ärenden som rör dataskyddslagstiftningen. Som exempel kan nämnas att det inte är lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärnverksamheten.

Det framhålls samtidigt att arbetet som dataskyddsombudet ställer höga krav vad avser **integritet** och **hög yrkesetik**.

Vad gäller erforderlig kompetens fastställer dataskyddsförordningen att ett dataskyddsombud **ska utses på grundval av yrkesmässiga kvalifikationer** och i synnerhet **sakkunskap om lagstiftning och praxis** avseende dataskydd samt förmågan att fullgöra ovan nämnda uppgifter.

4.3 Dataskyddsombud Alingsås kommun

Iakttagelser

I Alingsås kommun är dataskyddsombudet tillika digitaliseringsansvarig. Av intervjuerna med dataskyddsombudet framgår att digitaliseringsuppdraget upptar minst 80 % av tiden, där resterande 20 % ägnas uppgifterna som dataskyddsombud.

Kommentarer och bedömning

Utöver erforderliga kvalifikationer och kompetens ställer dataskyddsförordningen krav på att organisationen ska stödja dataskyddsombudet genom att tillhandahålla

erforderliga resurser. Det framhålls att dataskyddsombudet bör ha tillräckligt med tid i syfte att fullgöra sina uppgifter. Detta är särskilt viktigt när ett dataskyddsombud innehar flera funktioner och utses på deltid.

Vi anser att dagens upplägg med en kombinerad tjänst som digitaliseringsansvarig och dataskyddsombud inte är optimalt där tillägnad tid på ca 20 % inte är tillräcklig för uppdraget som dataskyddsombud för en kommun i Alingsås storlek.

Av intervju med dataskyddsombudet framkommer att det inte finns tid till att granska och kontrollera nämndernas och styrelsernas arbete, (vilket ska ske systematiskt), genomföra riktade utbildningsinsatser, kontinuerliga möten mellan dataskyddsombudet och förvaltningarna, kontinuerlig rådgivning mm. Av intervjuerna framgår att bristande tid och utrymme har lett till att fokus hamnar endast på ”hands-on” lösningar, exempelvis när en personuppgiftsincident inträffar.

Det framgår att det har funnits ambitioner att köpa tjänsten som dataskyddsombudet externt.

Bristande resurser återspeglas också i utbildningsinsatserna. Vad avser riktade utbildningar utifrån nämndernas särskilda behov har endast vård- och omsorgsnämnden erhållit en utbildning.

Vi bedömer att datasskyddombudet utifrån rådande tjänsteomfattning inte har möjlighet att agera rådgivande, bevaka och granska samt arbeta förebyggande.

Formellt sett förefaller befattningen digitaliseringsansvarig att ingå i kommunledningen, vilket kan medföra risker vad gäller oberoendefrågan. Dock framgår av intervjuerna att digitaliseringsansvaring i praktiken inte ingår i kommunledningsgruppen och organisationsledningen och är ej delaktig i att fatta strategiska beslut om kärnverksamheten.

Det bör beaktas att kommunstyrelsen har ett ansvar att tillse att det inte finns risker för intressekonflikter, beroendeposition mm. när rollen som dataskyddsombud kombineras med andra uppdrag i kommunen.

Vi anser sammantaget att uppdragets omfattning bör ses över samt utökas då vi bedömer dagens omfattning som otillräcklig.

5. Utnämning av dataskyddsombud

Samtliga personuppgiftsansvariga ska utse ett dataskyddsombud. Beslutet ska dokumenteras och vara protokollfört.

Iakttagelser

Vi har tagit del av samtliga nämnders beslut avseende utnämning av dataskydds-ombud.

Kommentarer och bedömning

Granskningen visar att samtliga nämnder formellt har utsett ett dataskyddsombud. Besluten är dokumenterade och protokollförda. Detta bedöms som positivt.

6. Personuppgiftsincidenter, konsekvensbedömning och dokumentation

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna innebär närmare att individer **förlorar kontrollen** över sina uppgifter eller att rättigheterna inskränks genom exempelvis **obehörigt röjande** av eller **obehörig åtkomst** till personuppgifter.

Dataskyddsförordningen, (artikel 33, punkt 1), fastställer att vid en personuppgifts-incident ska den personuppgiftsansvarige utan onödigt dröjsmål och inte senare än **72 timmar** efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. I Sverige är det Datainspektionen som är behörig tillsynsmyndighet.

Den registrerade ska informeras om personuppgiftsincidenten omedelbart, (artikel 34, punkt 1).

De personuppgiftsincidenter som inte bedöms medföra risker för individers rättigheter och friheter behöver ej anmälas till Datainspektionen. Därav är det av vikt att ansvarig nämnd genomför en konsekvensanalys vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

Samtliga personuppgiftsincidenter ska **dokumenteras oaktat allvarlighetsgraden**.

EU-rätten fastställer vidare att i de fall där organisationen har anlitat ett personuppgiftsbiträde, (PuB), ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige, (nämnd & styrelse), utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, (artikel 33, punkt 2).

Iakttagelser

Vi har tagit del av en rutinbeskrivning daterad 2018-09-20. Av rutinen framgår bl.a. att vid en personuppgiftsincident ska ansvarig chef tillsammans med utsedd kontaktperson för samordning av dataskyddsarbetet, kontakta dataskyddsombudet, där också en rapport om aktuell personuppgiftsincident ska upprättas och inlämnas till

dataskyddombudet. Ansvarig förvaltning ska genom utsedd samordnare diarieföra rapporten i kommunens ärendehanteringssystem.

Det fastställs vidare att dataskyddsombudet gör en bedömning om huruvida incidenten ska anmälas till Datainspektionen. Likaså ansvarar dataskyddsombudet för en bedömning om incidentetens allvarlighetsgrad som ligger till grund huruvida den registrerade ska informeras.

Vi har tagit del av upprättade rapporter avseende inträffade personuppgiftsincidenter som förvaltningarna ansvarar för att fylla i. Av rapportstrukturen framgår ett frågebatteri omfattande 11 frågor följt av information om anmälarens kontaktuppgifter. Dock råder det en oenhetlig tillämpning, där vissa delar inte finns med i en del rapporter.

Vidare förekommer olikartade tolkningar i förvaltningarna vad avser en del frågor så som:

- *Vilken typ av incident har inträffat?*
- *Vilka kategorier av registrerade berörs av incidenten?*
- *Vilka konsekvenser kan incidenten få?*

I rapportblanketten återfinns frågor avseende bedömningar om en incident ska anmälas till datainspektionen eller ej samt huruvida den registrerade ska informeras, där anmälaren ska redogöra för dessa bedömningar från förvaltningens sida.
Det är dock oklart huruvida det har skett ett samråd med dataskyddsombudet i dessa bedömningar.

Av intervjuerna framgår att förvaltningarna gör sina egna bedömningar vad gäller ovan nämnda punkter och att dataskyddsombudet bistår i bedömningarna vid behov.

Det råder vidare en oenhetlig hantering avseende vem som fyller i rapportblanketten.

Vi har noterat att det förekommer inkonsekventa bedömningar. Exemplevis finns incidenter där det framgår att konsekvenserna medför tydliga risker för den registrerades rättigheter och friheter men som har bedömts som ej allvarliga och därmed inte anmälts till Datainspektionen. Vidare har inte heller den registrerade informerats. Ett exempel är röjande av skyddade personuppgifter, där konsekvensen bedöms vara att den registrerade riskerar att komma till skada.
Lagstiftningens främsta intention med informationen till enskilda utan onödigt dröjsmål är att ge de registrerade specifik information om de åtgärder som de bör vidta för att skydda sig själva.

Vi har uppmärksammat avsaknaden av kontaktuppgifter till anmälaren i vissa rapporter samt förekomst av inkomplett rapport.

Ett fåtal incidenter har inrapporterats till datainspektionen. På frågan om vem som är personuppgiftsansvarig i anmälningsblanketten till Datainspektionen ska den **nämnd** där personuppgiftsincidenten har ägt rum anges, då det är nämnd och styrelse som är juridiskt sett personuppgiftsansvariga. De inrapporteringsunderlag som vi har tagit del av anges Alingsås kommun som personuppgiftsansvarig.

Nedan redogörs för antal personuppgiftsincidenter per nämnd. Vid tid för granskningen har vård- och omsorgsnämnden flest antal personuppgiftsincidenter. Detta kan bero på olika faktorer.

Figur 5:1

Nämnd	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI
Kommunstyrelsen	1	1	2	0
Barn-och ungdomsnämnden	0	0	4	2
Samhällsskyddsnämnden	0	0	1	0
Kultur- och utbildningsnämnden	0	0	1	0
Miljö- och hälsoskyddsnämnden	0	0	0	0
Tekniska nämnden	0	0	0	0
Socialnämnden	0	0	1	0
Vård- och omsorgsnämnden	5	0	9	1
Överförmyndarnämnden	0	0	0	0

Kommentarer och bedömning

Vi bedömer att det finns ett behov av en kunskapsökning i förvaltningarna samt bland personal ute på fältet vad gäller **hantering, dokumentation** och **risk- och konsekvensbedömning** av personuppgiftsincidenter. Detta i syfte att uppnå en enhetlig tolkning och förståelse i verksamheterna av dataskyddsförordningens krav och intentioner vad gäller personuppgiftsincidenter samt skapa förutsättningar för en korrekt hantering i den praktiska tillämpningen.

Under 2019 har Datainspektionen fått in ca 90 anmälningar per vecka och det är en ökning med ca 30 % i jämförelse med 2018. Ökningen härleds till en ökad medvetenhet och kunskap om anmälningsskyldigheten. Det bör också beaktas att det finns ett stort mörkertal avseende anmälningspliktiga incidenter som inte anmäls.

Vår bedömning är att sannolikheten att flertalet nämnder inte har haft någon form av personuppgiftsincident alternativt har endast ett fall, är låg. Som exempel kan nämnas att det är tillräckligt med att ett mail innehållande personuppgifter skickas till fel mottagare för att det ska klassas som en personuppgiftsincident.

Vad avser upptäckt samt redogörelse av incidenter kan en förklarande orsak avseende de nämnder som inte har angivit någon förekomst av personuppgiftsincidenter alternativt har endast inrapporterat enstaka fall, vara avsaknad av tillräcklig kunskap om vad en personuppgiftsincident är och vad som ska klassas som en incident. Övriga orsaker kan vara en ”rädsla” för offentliggörande av incidenter utanför den egna nämnden.

Denna bild delas av de intervjuade tjänstepersoner där det råder enighet om behovet av utbildningsinsatser vad gäller förståelse och hantering av personuppgiftsincidenter.

Vissa nämnder har också kommit längre i sitt arbete vad gäller kunskap, bedömning och hantering av förekommande incidenter, vilket leder till att en högre andel personuppgiftsincidenter upptäcks samt inrapporteras.

Vi anser att det finns ett behov av att förvaltningarna samt personal ute på fältet får en närmare information om klassning av personuppgiftsincidenter, där utveckling av begreppet följt av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

Dokumentation av personuppgiftsincidenter är obligatorisk, där den personuppgifts-ansvarige ska dokumentera samtliga personuppgiftsincidenter inbegripet **omständigheterna kring incidenten**, **risker** och **effekter** samt de **korrigerande åtgärder** som har vidtagits. Detta innebär att respektive personuppgiftsansvarig ska genomföra en risk- och konsekvensbedömning följt av en tydlig dokumentation.

Dokumentation ska ske oaktat om nämnden bedömer att inrapportera personuppgiftsincidenten till Datainspektionen eller ej.

Det bör framhållas att personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter samt förtroendeskador för Alingsås kommun.

Dokumentationen ska bl.a. göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av hantering av personuppgiftsincidenter.

Vi anser att det finns ett behov av ett omtag avseende dokumentation av personuppgiftsincidenter, där det finns ett behov av en ökad central styrning vad gäller övergripande styrdokument följt av mallar/inrapporteringsblanketter. Vi bedömer att dokumentationen av förekommande incidenter under 2019 inte är på en tillfredställande nivå, då dokumentationen är bristfällig.

Grundläggande förutsättningar

Den nu gällande rapportblanketten behöver bl.a. formaliseras där exempelvis grundläggande information så som ”kommunnamn” bör framgå. Blanketten behöver vidare kompletteras med väsentliga delar. Två viktiga delar som bör tillföras blanketten är information om vem som är personuppgiftsansvarig samt inom vilket verksamhets-område incidenten har inträffat. Uppgift om vilken nämnd/styrelse som är personuppgiftsansvarig ska finnas med i blanketten.

Rapportstrukturen omfattar vissa delar som ingår i Datainspektionens anmälnings-blankett. Flertalet kommuner använder sig av **Datainspektionens anmälnings-blankett** för dokumentation av personuppgiftsincidenter, där frågorna i sin helhet har förts över till en kommunanapassad blankett. Vi rekommenderar Alingsås kommun att göra detsamma i syfte att uppnå en enhetlig hantering inom verksamheterna samt få med samtliga viktiga delar.

Det är vidare av vikt att det finns **svarsalternativ** att tillgå vid centrala frågor, i syfte att undvika feltolkningar inom verksamheterna vid dokumentation och inrapportering av en incident. Lämpliga svarsalternativ finns i datainspektionens mall.

För att uppnå en korrekt dokumentation samt kunna genomföra en underbyggd risk- och konsekvensbedömning följt av bedömning om lämpliga och korrekta åtgärder behöver blanketten kompletteras till att omfatta följande delar:

- Kommunnamn
- Information om personuppgiftsansvarig
- Inom vilket verksamhetsområde har incidenten inträffat med syfte på kommunens interna verksamhetsorganisation (t.ex.: Elevhälsa, förskola/grundskola/gymnasieskola, plan- och bygglov, hemsjukvård, IFO etc.)
- När inträffade incidenten, (Idag finns enbart frågan om när incidenten har upptäckts. Incidentetens tidpunkt samt upptäckt kan ske vid skilda tidsperioder och har betydelse för att kunna efterleva lagrummet om anmälan inom 72 timmar)
- Frågan om ”vilken typ av incident som har inträffat” bör kompletteras med följande svarsalternativ i syfte att undvika misstolkningar: *Obehörigt röjande, Obehörig åtkomst, Förlust av information, Förstöring av information, Ändring*.
- Hur har incidenten upptäckts, följt av svarsalternativ.
- Varför incidenten har inträffat, följt av svarsalternativ (Tekniskt fel, säkerhetsbrister, dataintrång, brist i rutinerna, mänsklig faktor mm.) Denna information är av vikt för att kunna vidta korrekta åtgärder samt införa förebyggande rutiner.
- Huruvida incidenten gäller personuppgifter som hanteras av **personuppgiftsbiträden**. I dessa fall behöver personuppgiftsansvarig tillse att biträdet utan dröjsmål vidtar lämpliga åtgärder för att minimera konsekvenserna av incidenten.
- Information om eventuella personuppgiftsbiträden.
- Huruvida uppgifterna var krypterade
- Frågan om ”vilka kategorier av registrerade berörs av incidenten” kan kompletteras med svarsalternativ i syfte att tydliggöra innebörden.
- Frågan om ”vilka kategorier av personuppgifter berörs av incidenten” bör kompletteras med svarsalternativ.
- Frågan om ”vilka konsekvenser kan incidenten få” bör kompletteras med svaralaternativ.
- Allvarlighetsgrad, dvs. en bedömning om hur allvarlig incidenten är. Följande svarsalternativ bör tillföras blanketten: *Obetydlig, Begränsad, Betydande, Mycket allvarlig.*
- Åtgärder med anledning av incidenten följt av information om när i tid åtgärderna har satts in.

- Motivering till varför de registrerade ev. inte kommer att informeras.

Som tidigare nämnts bör möjliga svarsalternativ anges vid frågorna i syfte att underlätta ifyllandet av rapporten för anmälaren. Svarsalternativen kan hämtas från Datainspektioners anmälningsblankett.

Blanketten bör vid förekommande fall av incidenter kompletteras med ett förvaltningsbeslut om huruvida personuppgiftsincidenten ska inrapporteras till Datainspektionen eller ej. Blanketten inklusive ett beslut bör diarieföras.

Det bör noteras att anmälan till Datainspektionen är obligatorisk, såvida det inte är sannolikt att incidenten leder till en hög risk för fysiska personers rättigheter och friheter. Detsamma gäller information till de registrerade.

Dataskyddsombudets främsta uppdrag är att övervaka efterlevnaden av dataskyddsförordningen följt av rådgivning och stöd till personuppgiftsansvariga nämnder och bolagsstyrelser. Härigenom är det av vikt att information om uppkomna personuppgiftsincidenter kommer till dataskyddsombudets kännedom.

Vad avser den kommunövergripande rutinbeskrivningen kan den med fördel innehålla en beskrivning om **vilken information som ska ges till den registrerade** vid en incident som medför en hög risk för de registrerades rättigheter och friheter. Centrala delar är: en klar och tydlig beskrivning av incidenteten, kontaktuppgifter till dataskyddsombudet samt den person som är insatt i ärendet, beskrivning av sannolika konsekvenser av incidenteten samt åtgärder som har vidtagits följt av beskrivning av insatser som har genomförts för att mildra konsekvenserna.
Denna information som en del i ett kommunövergripande styrdokument minimerar riskerna med olikartade tillämpningar i verksamheterna.

Sammanfattningsvis rekommenderar vi att kommunstyrelsens ledamöter årligen får ta del av en statistik avseende samtliga inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt. I dagsläget når inte informationen till kommunstyrelsen i sin helhet.

7. Registerförteckningar

I enlighet med dataskyddsförordningen, artikel 30, ska varje personuppgiftsansvarig föra ett register över personuppgiftsbehandling som utförts under dess ansvar bestående av följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall den personuppgiftsansvariges företrädare.
- Namn och kontaktuppgifter till dataskyddombud.
- Ändamålen med behandlingen.
- Beskrivning av kategorierna av registrerade.

- Beskrivning av kategorierna av personuppgifter
- Förekomst av särskilda kategorier av personuppgifter (känsliga personuppgifter)
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer, (kategorier av mottagare av personuppgifter internt och externt).
- Överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Tidsfristerna för radering av de olika kategorierna av uppgifter.
- Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.
- Laglig grund för behandlingen.
- Förekomst av anlitande av personuppgiftsbiträden.

Registerförteckningarna ska på begäran redovisas för tillsynsmyndigheten, dvs. Datainspektionen

Iakttagelser

Av granskningen framkommer att nämnderna har upprättat registerförteckningar över viss del av personuppgiftsbehandlingar. Dock finns väsentliga brister.

Vid tid för granskningen saknas registerförteckningar för behandlingar inom kommunikationsenheten samt säkerhetsenheten som lyder under kommunstyrelsen.

Aktuell mall för registerförteckningarna har arbetats fram under 2017 och är i wordformat, vilket inte är lämpligt för detta ändamål utifrån den mängd information som behöver tillföras registerföreteckningen. Barn- och ungdomsnämnden, vård- och omsorgsnämnden samt HR-avdelningen och ekonomienheten som lyder under kommunstyrelsen använder sig av programmet Excel som är mer lämpat för detta ändamål.

Av intervjuerna framgår att vissa nämnder har tillfört ytterligare frågeställningar och information i ursprungsmallen som kan vara av värde men som i sin tur har orsakat en oenhetlighet.

Som tidigare nämnts har dataskyddsombudet bl.a. till uppgift att övervaka efterlevnaden av hantering av personuppgifter. Detta ska ske bl.a. genom systematiska granskningar. Ett första granskningsområde bör vara registerförteckningarna. Vid tid för granskningen finns ingen uttalad granskningsplan för Alingsås kommuns nämnder och bolag följt av dokumenterade granskningsrapporter. Som tidigare nämnts är dessa insatser inte möjliga mot bakgrund av rådande tjänsteomfattningsgrad för dataskyddsombudet.

Av intervju med dataskyddsombudet råder det en enighet vad gäller bedömning om att registerförteckningarna är bristfälliga. Det framgår också att det finns ett behov av kunskapsökning vad gäller hantering av registerförteckningar som är en central del i efterlevnaden av dataskyddsförordningen.

Vad avser mallstrukturen i registerförteckningarna återfinns ett frågebatteri som ska besvaras vid varje personuppgistbehandling. Utifrån utrymmesskäl pga. felval av IT-verktyg, har flera frågor slagits samman i frågefälten vilket leder till svårigheter vid ifyllande av svar, uppföljning, uppdatering, återsökning samt tillsyn.

Vi har genomfört en övergripande granskning av nämndernas registerförteckningar, där granskningen visar att det finns en del brister där följande förekommer:

- Avsaknad av personuppgiftsansvarig. Bör beaktas att det är nämnd eller styrelse som juridiskt sett är ytterst ansvarig för efterlevnad av dataskyddsförordningen, där enskilda anställda inte kan anges som personuppgiftsansvariga.

- Avsaknad av namn och kontaktuppgifter till dataskyddsombud

- Avsaknad av namn och kontaktuppgifter till personuppgistansvariges företrädare. Namnuppgifter återfinns i vissa fall, dock saknas kontaktuppgifter. Förekomst av endast förnamn. Vidare förekommer att en ”enhet/avd.” anges som kontaktperson.

- Varje personuppgiftsbehandling ska anges självständig följt av separata svar vad avser exempelvis: ändamål, rättslig grund, kategorier av registrerade, typer av personuppgifter, samtycke, personuppgiftsbiträde, personuppgiftsbiträdesavtal, överföring till tredje land, förekomst av känsliga personuppgifter, konsekvensbedömning, informationsplikt, tidsfrist för radering, tekniska och organisatoriska säkerhetsåtgärder mm. Dock förekommer fall där nämnderna har slagit ihop flera personuppgiftsbehandlingar. Som exempel kan socialnämnden nämnas där ca 50 olika personuppgiftsbehandlingar redogörs som en enda behandling, vilket är bristfälligt samt allvarligt utifrån bl.a. att behandlingarna innehåller sekretessbelagd information, (t.ex. *boendestöd, placeringar, arbetsförmågebedömningar, dödsbo, ekonomi, externa placeringar vuxna, lägenheter som socialnämnden hyr, planering ensamkommande barn, HVB, köpt vård, familjerättsenhet, Hälsoteket, sekretessmaterial, socialadministratör barn och unga, sekretessrum för familjehemssekr., utredning EKB, utredningar, återkrav* mm).
Som tidigare nämnts innehåller de sammanslagna personuppgiftsbehandlingarna sekretessbelagd information, dock har det i registerförteckningen angivits att särskilda kategorier av uppgifter ej förekommer.

- Sammanslagning av olika personuppgiftsbehandlingar förekommer även inom miljöskyddsnämnden samt samhällsbyggnadsnämnden, där dessa benämns bl.a. som ”diverse listor”. Av granskning av samhällsbyggnadsnämndens registerförteckning framgår en sammanslagning av åtta olika behandlingar: *Radon, hygienisk behandling, tillsyn fastighetsägare, undervisningslokaler, äldreboende och vårdlokaler, vedeldning och strandskydd*, vilket strider mot gällande lagstiftning. Uppgifterna anges finnas under en gemensam filyta G:, vilket möjliggör obehörig åtkomst. Vidare är lagring av personuppgifter i form av ostrukturerat material inte tillåtet.

- Avsaknad av kategorier av registrerade, där **kategorier** av personer som blir registrerade ska framgå, t.ex.: medarbetare, elever, sökande avseende försörjningsstöd, biståndsbedömning, låntagare på biblioteket m.fl.
I registerförteckningarna återfinns ovannämnda frågeställning, dock har frågan misstolkats, där **typ av personuppgifter** anges istället. Kommunstyrelsen bör tillse att det finns två separata kolumner innehållande följande frågeställningar i mallstrukturen för registerförteckningar:
Vilka kategorier av registrerade behandlas?
Vilka typer av personuppgifter behandlas?

- Avsaknad av angivelse av laglig/rättslig grund för registreringen.
Den lagliga grunden som personuppgiftsbehandlingen stödjer sig mot ska anges med aktuellt lagrum, dvs. artikelnummer i GDPR samt kapitel och paragraf i de fall där behandlingen stöds med hjälp av en nationell speciallagstiftning. Begrepp som speciallagstiftning, grundlag, lagstöd för grundläggande stöd etc. kan en anges som laglig grund, utan ska specificeras i form av aktuell lag följt av aktuellt lagrum.

Vi vill också framhålla att ”intresseavvägning” kan ej användas inom kommunal verksamhet och kan därmed inte anges som rättslig grund för en personuppgiftsbehandling.

- Vad avser så kallade ”särskilda kategorier av personuppgifter”, (känsliga personuppgifter), är det lämpligt att en självständig kolumn ägnas detta område med följande formulering: Behandlas känsliga uppgifter och vilka? Följt av en fråga om lagstöd.
Utgångspunkten är att det är förbjudet att behandla känsliga personuppgifter. Det finns dock undantag, exempelvis när någon lämnar in sitt samtycke till att känsliga uppgifter får behandlas. För att behandla känsliga personuppgifter krävs lagstöd antingen i **dataskyddsförordningen** eller genom **nationell lagstiftning.**
Vad avser behandling av känsliga personuppgifter finns specificerade krav enligt artikel 9 i dataskyddsförordningen följt av **krav på konsekvensbedömningar** i enlighet med artikel 35. Detta ställer krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade samt stödjas av en rättslig grund. Samtliga nämnder bör se över huruvida detta krav har uppfyllts. Denna del har ej ingått i granskningen.

I mallstrukturen efterfrågas huruvida känsliga personuppgifter behandlas samt vilket lagstöd som används. Dock saknas denna information vid flertalet personuppgifts-behandlingar.

- Avsaknad av svar om huruvida nämnden uppfyller kraven om information till den registrerade.

- Avsaknad av allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

- Avsaknad av tidsfrister för gallring. Bör framhållas att vad avser angivande av tidsfrister ska dessa anges uttryckligen, dvs. det räcker inte med en hänvisning till nämndens dokumenthanteringsplan. Denna punkt berör dataskyddsförordningens grundläggande princip om ”lagringsminimering”.

- Avsaknad av information om överföring till tredje land.

- Avsaknad av information om samtycke samt rutiner om detsamma. Svar förekommer där det anges att samtycke ej behövs utifrån ”lagligt stöd”, dock saknas uppgifter om aktuell lagstiftning och lagrum.

- Vi har uppmärksammat att förvaltningarna har svarat med ”vet ej” alt. ”inget svar” samt ”frågetecken” i flertalet fall avseende vissa kategorier av frågor i registerförteckningarna.

- Senaste revideringsdatum bör framgå av registerförteckningen. Vid tid för granskningen har kultur- och utbildningsnämnden samt miljöskyddsnämnden angivit denna information.

Vi har vidare noterat att Vård och omsorgsnämnden har skapat en ”egen” mall vad avser registerförteckningar, dock saknas flertalet obligatoriska samt viktiga frågeställningar.

Vi har uppmärksammat att den nämnd som har kommit längst vad gäller själva mallstrukturen i registerförteckningar över nämndens personuppgiftsbehandlingar är barn- och ungdomsnämnden där förvaltningen har skapat en ”egen” mall bestående av både obligatoriska frågeställningar men också andra viktiga frågeställningar som är av värde för nämndens interna arbete vad gäller efterlevnad av dataskyddsförordningen. Ytterligare frågefällt som behöver tillföras mallen är namn och kontaktuppgifter till **dataskyddsombud** samt namn och kontaktuppgifter till den **leverantör som anlitas som personuppgiftsbiträde.**

Likaså har kultur- och utbildningsnämnden kommit längre vad gäller struktur och innehåll i registerförteckningarna. De frågeställningar som behöver tillföras mallen för registerförteckningen är: Personuppgiftsansvarig, Huruvida det förekommer överföring till tredje land, samt Huruvida personuppgiftsbiträde anlitas följt av namn och kontaktuppgifter till biträdet.

Överförmyndarnämnden bör tillse att det finns registerförteckningar över samtliga personuppgiftsbehandlingar. Vid tid för granskningen innehåller överförmyndarnämndens registerförteckning endast två personuppgiftsbehandlingar vilket är bristfälligt. Som exempel kan nämnas att registerförteckningar bör finnas för: Anhörigregister, register över ställföreträdare, ansökan om samtyck till fördelning enligt arvskifte, ansökan om uttag överförmyndarspärrat konto, samtycke mm.

Övriga nämnder bör också sondera huruvida registerförteckningar finns för samtliga behandlingar.

Kommentarer och bedömning

Vi bedömer att det krävs ett omtag vad avser arbetet med registerförteckningar. Det bör betonas att detta arbete är än mer viktigt för de nämnder som har en myndighetsutövande funktion.

Det finns ett behov av översyn av strukturen i registerförteckningarna där den behöver revideras i sin helhet.

Ett första steg bör därmed vara revidering av nuvarande mall för registerförteckningar vad gäller struktur och frågeställningar. Granskningen visar att utifrån befintliga brister i mallen har vissa nämnder skapat ”egna varianter”.

Vi bedömer att det är av vikt att det finns uppdaterade kommunövergripande styrdokument följt av korrekta mallar och underlag avseende hantering av personuppgifter. Detta i syfte att bl.a. uppnå en enhetlig nivå och hantering av behandling av personuppgifter inom verksamheterna.

Vi bedömer att det finns ett tydligt behov av utbildningsinsatser vad avser register-förteckningar som är grundstommen i hanteringen av personuppgifter.

Det bör noteras att respektive nämnd och styrelse är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Dock ska kommunstyrelsen inom ramen för sin uppsiktsplikt följa upp huruvida nämnder och bolagsstyrelser hanterar det ålagda ansvaret följt av centrala styrdokument som stödjer verksamheterna i dataskyddsarbetet.

Vi ser det som positivt att kommunstyrelsens ansvar har förtydligats i det kommunövergripande styrdokumentet för behandling av personuppgifter, (antaget av Kf 2019-04-24 § 79), där det framgår att kommunstyrelsen ska säkerställa att kommunens arbete med efterlevnad av dataskyddsförordningen sker på ett korrekt och samordnat sätt.

Registerförteckningarna ska uppdateras vid behov och hållas aktuella. Nämnderna har ett ansvar att tillse att **samtliga** behandlingar upptas i en registerförteckning. Härigenom bör förvaltningarna sondera huruvida det finns personuppgiftsbehandlingar som inte finns registrerade.

Vidare bör dataskyddsombudet genomföra dokumenterade granskningsinsatser för respektive nämnd och bolag. Resultatet följt av rekommendationer bör dokumenteras i en granskningsrapport för varje nämnd och styrelse.

Vi rekommenderar att dataskyddsombudet upprättar en årlig granskningsplan med de granskningsinsatser som ska genomföra under året. Detta leder till att nämnderna kan förbereda sig samt i god tid förstå vad som förväntas av verksamheterna.

8. Övriga iakttagelser utanför ramen för revisionsfrågorna

Ostrukturerad data

Innan dataskyddsförordningen trädde i kraft fanns stöd i nationell lagstiftning, (Personuppgiftslag1998:204) som innebar enklare regler för hantering av personuppgifter i ostrukturerat material. Detta ”undantag” finns ej längre i och med dataskyddsförordningens ikraftträdande, där samma förskrifter gäller för alla personuppgifter.

Iakttagelser

Av intervjuerna framgår att det finns stora utmaningar vad gäller ostrukturerad data inom samtliga nämnder.

Vid tid för granskningen finns en gemensam filyta, där bl.a. en mängd personuppgifter har lagrats under en längre period, där stickprovskontroller genomförda av dataskyddsombudet har visat att det bl.a. finns bilder, film, kalkyldokument, ordbehandlingsdokument som innehåller olika typer av personuppgifter.

Av erhållen kontrolldokumentation framgår att filytan används gemensamt av verksamheterna, där stora delar är tillgänglig för alla anställda i kommunen. Det finns vidare äldre dokument som har skapats av före detta anställda, där behovet och aktualiteten behöver sonderas.

Dataskyddsombudet har lyft och uppmärksammat kommunledningen på ovanstående.

I samband med granskning av registerförteckningarna har vi noterat att filytan också används för hantering av diverse block av personuppgiftsbehandlingar.

Kommentar och bedömning

Den gemensamma filytan bör ses över snarast, där hanteringen strider mot gällande lagstiftning.

Aktuella uppgifter som behöver behandlas ska flyttas över till lämpligt system i respektive nämnd. Det bör betonas att behandling kan endast ske med stöd av en rättslig grund följt av befogat ändamål. Övriga uppgifter ska gallras.
En av de grundläggande principerna är lagringsminimering, vilket innebär att personuppgifter ska raderas när de inte längre behövs.

Det bör vidare betonas att personuppgifter får endast samlas in och behandlas för specifika, särskilda uttryckligt angivna, konkreta och berättigade ändamål.

Vidare ska samtliga personuppgifter skyddas från obehörig åtkomst, vilket innebär att det ska finnas behörighetsbegränsningar samt behörighetskontroller, där tillgång till visst block av personuppgiftsbehandlingar ska begränsas till behörig personal inom respektive nämnd och verksamhetsområde. Det bör betonas att varje styrelse/nämnd är en ”egen” myndighet med ansvar för hantering av personuppgifter.

Ovan nämnda åtgärder bör genomföras snarast.

Det finns vidare lokala lagringsutrymmen, där anställda kan ha lagrat personuppgifter. Vi rekommenderar att samtliga anställda uppmanas att se över lokala lagringsutrymmen för att antingen flytta nödvändiga uppgifter för arbetet, till rätt plattform eller gallra. Som tidigare nämnts kan personuppgifter endast behandlas med stöd av rättsliga grunder för specifika och berättigande ändamål.

9. Registerutdrag, rättelse och radering

I enlighet med dataskyddsförordningen har den registrerade rätt att begära ut ett så kallat registerutdrag från offentliga och privata organisationer. Ett registerutdrag ska redogöra för de personuppgifter som en myndighet eller ett företag behandlar om en person samt på vilket sätt uppgifterna behandlas.

Likaså har den registrerade rätt till att utan dröjsmål få felaktiga uppgifter rättade. På samma sätt finns rättigheten att utan onödigt dröjsmål få sina personuppgifter raderade om de inte längre är nödvändiga för de ändamål för vilka de samlats in eller att den registrerade återkallar sitt samtycke som behandlingen grundar sig på. Den registrerade kan också invända mot registreringen utifrån att det saknas en laglig grund eller berättigade skäl för behandlingen. Ett exempel är direkt marknadsföring.

Iakttagelser

Vi har tagit del av kommunens rutinbeskrivning vad avser rutin för utlämnande av registerutdrag, (antagen av Kf 2020-09-04). Dock saknas dokumenterade rutiner avseende begäran om rättelse och radering.

Kommentarer och bedömning

Kommunstyrelsen bör upprätta en dokumenterad rutinbeskrivning avseende rättelse och radering av personuppgifter. Av rutinen bör ansvarsfördelning samt praktiskt utförande vid en eventuell begäran om rättelse eller radering framgå.

Vi rekommenderar att specifika e-blanketter arbetas fram för rättelse och radering i syfte att underlätta för de registrerade samt effektivisera genomförandeprocessen inom verksamheterna genom att exempelvis minimera behovet av kompletteringar mm.

KPMG AB

Viktoria Bernstam
Specialist/Certifierad kommunal revisor